UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,475	04/16/2004	G. Glenn Henry	CNTR.2223	1510

23669 7590 04/23/2007 HUFFMAN LAW GROUP, P.C. 1900 MESA AVE. COLORADO SPRINGS, CO 80906	**EXAMINER** ZEE, EDWARD

ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/23/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/23/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

PTOL-90A (Rev. 10/06)

	Application No.	Applicant(s)
Office Action Summary	10/826,475	HENRY ET AL.
	Examiner	Art Unit	
	Edward Zee	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *16 April 2004*.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-33* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-33* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *16 April 2004* is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *See Continuation Sheet*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :4/16/04,4/16/05,9/25/05,3/11/06,3/18/06,6/4/06,7/25/06,9/30/06,11/3/06,1/25/07,3/19/07,3/26/07,4/10/07.

DETAILED ACTION

1.   This action is in response to the original filing of April 16th, 2004. Claims 1-33 are

pending and have been considered below.

Specification

2.   The disclosure is objected to because of the following informalities: the examiner notes

the use of acronyms (ie. IEEE, RSA, USB, etc.) throughout the specification without first

including a description in plain text as required.

3.   The disclosure is objected to because it contains an embedded hyperlink and/or other

form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or

other form of browser-executable code. See MPEP § 608.01.

4.   The use of the trademark Linux® has been noted in this application. It should be

capitalized wherever it appears and be accompanied by the generic terminology.

        Although the use of trademarks is permissible in patent applications, the proprietary

nature of the marks should be respected and every effort made to prevent their use in any manner

which might adversely affect their validity as trademarks.

        Appropriate correction is required.

Claim Objections

5.   Claims 9 and 33 are objected to because of the following informalities: the examiner

notes the use of acronym "x86" in the claims without first including a description in plain text as

required. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
> subject matter which the applicant regards as his invention.

7.   Claim 13 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention. The examiner notes that it is unclear what "a number blocks" means. It appears

that the applicant is attempting to claim, indicating "a number of blocks", and will interpret the

claim in this manner.

Claim Rejections - 35 USC § 102

8.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

9.   Claims 1-8, 10-12, 14-25, and 27-32 are rejected under 35 U.S.C. 102(e) as being

anticipated by Yup et al. (2002/0191784).

Claim 1: Yup et al. discloses an apparatus for performing cryptographic operations, comprising:

        a. a cryptographic instruction, received by a computing device as part of an instruction

flow executing on said computing device, wherein said cryptographic instruction prescribes one

of the cryptographic operations, and wherein said cryptographic instruction prescribes one of a

plurality of cryptographic key sizes*(AES block cipher can use varying key lengths)* [page 4,

paragraph 0045];

b. and execution logic, operatively coupled to said cryptographic instruction, configured

to execute said one of the cryptographic operations, said execution logic comprising: a key size

controller*(key expansion block)*, configured to employ said one of a plurality of cryptographic

key sizes during execution of said one of the cryptographic operations [page 3, paragraph 0028].

Claims 2 and 3: Yup et al. discloses an apparatus as in claim 1 above and further discloses that

said one of the cryptographic operations further comprises an encryption and decryption

operation, said encryption operation comprising encryption of a plurality of plaintext

blocks*(plurality of channels with input means)* to generate a corresponding plurality of ciphertext

blocks*(plurality of channels with output means)* and said decryption operation comprising

decryption of a plurality of ciphertext blocks*(plurality of channels with input means)* to generate

a corresponding plurality of plaintext blocks*(plurality of channels with output means)* [page 2,

paragraph 0017.

Claims 4-6: Yup et al. discloses an apparatus as in claim 1 above and further discloses that said

one of a plurality of cryptographic key sizes comprises 128 bits, 192 bits and 256 bits [page 4,

paragraph 0045].

Claim 7: Yup et al. discloses an apparatus as in claim 1 above and further discloses that said one

of the cryptographic operations is executed according to the Advanced Encryption Standard

(AES) algorithm [page 2, paragraph 0016].

Claim 8: <u>Yup et al.</u> discloses an apparatus as in claim 1 above and further discloses that said key

size controller*(key expansion block)* is configured to interpret a key size field*(nk = key size)*

within a control word which is referenced by said cryptographic instruction*(the key expansion*

block generates a single round key by performing a single key expansion operation for each

round of the AES block cipher) [page 3, paragraph 0028].

Claims 10-12: <u>Yup et al.</u> discloses an apparatus as in claim 1 above and further discloses that

said cryptographic instruction implicitly references a plurality of registers, which include a first

register, wherein contents of said first register*(plaintext storage registers)* comprise a first

pointer to a first memory address, said first memory address specifying a first location in

memory for access of a plurality of input text blocks upon which said one of the cryptographic

operations is to be accomplished [page 4, paragraph 0043]; and a second register*(cipher block*

output storage register), wherein contents of said second register comprise a second pointer to a

second memory address, said second memory address specifying a second location in said

memory for storage of a corresponding plurality of output text blocks, said corresponding

plurality of output text blocks being generated as a result of accomplishing said one of the

cryptographic operations upon a plurality of input text blocks [page 4, paragraphs 0043-0044].

Claim 14: <u>Yup et al.</u> discloses an apparatus as in claim 10 above and further discloses that said

plurality of registers comprises a fourth register*(cipher key storage register)*, wherein contents of

said fourth register comprise a third pointer to a third memory address, said third memory

address specifying a third location in memory for access of cryptographic key data for use in

accomplishing said one of the cryptographic operations [page 3, paragraph 0028].

Claim 15: Yup et al. discloses an apparatus as in claim 14 above and further discloses that said cryptographic key data comprises a cryptographic key comprising a number of bits according to said one of a plurality of cryptographic key sizes [page 4, paragraph 0045].

Claim 16: Yup et al. discloses an apparatus as in claim 14 above and further discloses that said cryptographic key data comprises a user-generated cryptographic key schedule *(round key algorithm)* [page 3, paragraph 0028]. The examiner notes that it is inherent for the key schedule to be stored in memory if the key expansion block uses it to generate round keys.

Claim 17: Yup et al. discloses an apparatus as in claim 10 above and further discloses that said plurality of registers comprises a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations [page 3, paragraph 0027]. The examiner notes that Yup et al. discloses operating the apparatus in CBC mode, which implies the use of initialization vectors. Thus, it is inherent for the initialization vectors to be stored in memory.

Claim 18: Yup et al. discloses an apparatus as in claim 10 above and further discloses that said plurality of registers comprises a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises: a key size field *(nk = key*

size), configured to specify said one of a plurality of cryptographic key sizes to be employed

during execution of said one of the cryptographic operations*(the key expansion block generates a*

single round key by performing a single key expansion operation for each round of the AES

block cipher) [page 3, paragraph 0028]. The examiner notes that it is inherent for the control

word to be stored in memory because the key expansion block uses it for generating a round key.

Claim 19: Yup et al. discloses an apparatus as in claim 1 above and further discloses that said

execution logic comprises a cryptography unit, configured execute a plurality of cryptographic

rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality

of output text blocks, wherein said one of a plurality of cryptographic key sizes is prescribed by a

control word that is provided to said key size controller within said cryptography unit [page 1,

paragraph 0004].

Claim 20: Yup et al. discloses an apparatus for performing cryptographic operations,

comprising:

        a. a cryptography unit within a device, configured to execute one of the cryptographic

operations responsive to receipt of a cryptographic instruction within an instruction flow that

prescribes said one of the cryptographic operations, wherein said cryptographic instruction also

prescribes a key size to be employed when executing said one of the cryptographic

operations*(AES block cipher can use varying key lengths)* [page 4, paragraph 0045];

        b. and key size control logic*(key expansion block)*, operatively coupled within said

cryptography unit, configured to direct said device to employ said key size when performing said

one of the cryptographic operations [page 3, paragraph 0028].

Claims 21-23: <u>Yup et al.</u> discloses an apparatus as in claim 20 above and further discloses that

said key size comprises 128-bits, 192-bits and 256-bits [page 4, paragraph 0045].

Claim 24: <u>Yup et al.</u> discloses an apparatus as in claim 20 above and further discloses that said

one of the cryptographic operations is executed according to the Advanced Encryption Standard

(AES) algorithm [page 2, paragraph 0016].

Claim 25: <u>Yup et al.</u> discloses an apparatus as in claim 20 above and further discloses that said

key size control logic*(key expansion block)* is configured to interpret a key size field*(nk = key*

size) within a control word which is referenced by said cryptographic instruction [page 3,

paragraph 0028].

Claim 27: <u>Yup et al.</u> discloses a method for performing cryptographic operations in a device, the

method comprising:

    a. receiving a cryptographic instruction that prescribes cryptographic key size for

employment during execution of one of a plurality of cryptographic operations*(AES block cipher*

can use varying key lengths) [page 4, paragraph 0045];

    b. and employing the cryptographic key size*(key expansion block uses "nk", the key size,*

to generate a round key) when executing the one of the cryptographic operations [page 3,

paragraphs 0028-0035].

Claim 28: <u>Yup et al.</u> discloses a method as in claim 27 above and further discloses that said

receiving comprises via a field*(nk = key size)* within a control word that is referenced by the

cryptographic instruction, specifying the cryptographic key size [page 3, paragraph 0028].

Claims 29-31: Yup et al. discloses a method as in claim 28 above and further discloses that said

specifying comprises prescribing 128 bits, 192 bits and 256 bits as the cryptographic key size

[page 4, paragraph 0045].

Claim 32: Yup et al. discloses a method as in claim 27 above and further discloses that said

employing comprises executing the one of the cryptographic operations according to the

Advanced Encryption Standard (AES) algorithm [page 2, paragraph 0016].

Claim Rejections - 35 USC § 103

10.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

11.   Claims 9, 13, 26 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Yup et al. (2002/0191784).

Claims 9, 26 and 33: Yup et al. discloses an apparatus as in claims 1, 20 and 27 above and

further discloses that said cryptographic instruction is prescribed according to the x86 instruction

format. However, it would have been obvious to one of ordinary skill in the art at the time of

invention to create the instructions in x86 format or any other format. One would have been

motivated to do so in order to conform to the type of platform selected for implementation of the

encryption/decryption device.

Claim 13: Yup et al. discloses an apparatus as in claim 10 above, but does not explicitly disclose

that said plurality of registers comprises a third register, wherein contents of said third register

indicate a number of blocks*(channels)* within a plurality of input text blocks*(plurality of channels)* [page 2, paragraph 0016]. However, it would have been obvious to one of ordinary skill in the art at the time of invention to store the number of blocks being encrypted or decrypted. One would have been motivated to do so in order recognize when the entire encryption or decryption process is complete.

Conclusion

12.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Verbauwhede (2003/0202658), Zakiya (2001/0050989), Feldman et al. (2004/0047466) and Kim (6,246,768).
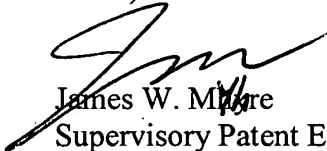
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 6:30AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James W. Myhre can be reached on (571) 270-1065. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
April 9, 2007

James W. Moore
Supervisory Patent Examiner

***